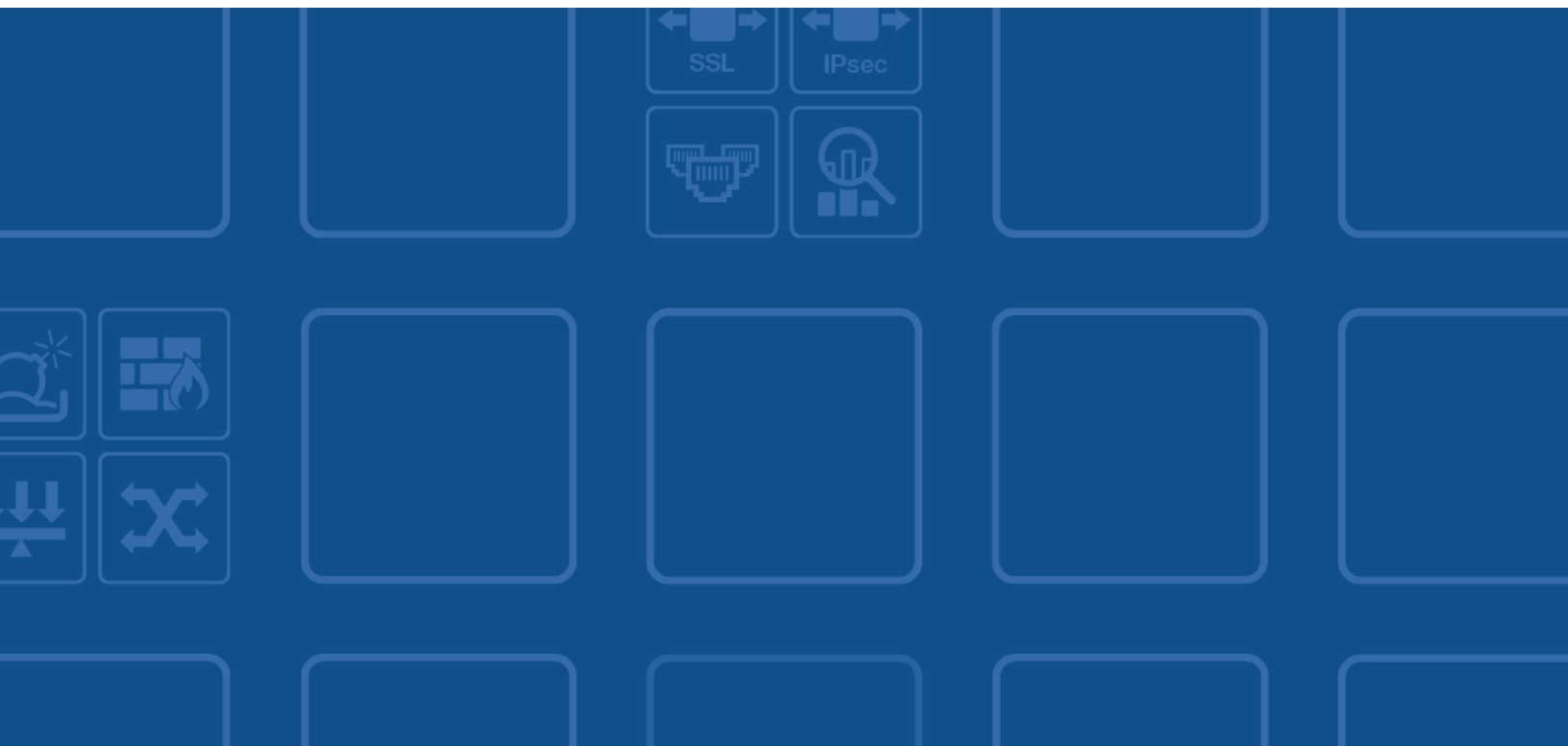
FORTINET
High Performance Network Security

FortiManager - Secure DNS Guide

VERSION 5.4.2



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

December 14, 2016

FortiManager 5.4.2 Secure DNS Guide

02-542-371653-20161214

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-12-14	Initial release

Introduction

Users are now able to enable FortiManager as a secure FortiGuard DNS server. Users can use this DNS server for web requests instead of using a public DNS server such as Google.

FortiManager Secure DNS provides regular DNS name resolving and DNS ratings (hostname ratings). When the rating is malicious or suspicious, FortiManager Secure DNS redirects the client's HTTP request, with warning messages, to a custom web portal.

When the SDNS license is applied to FortiManager, FortiManager switches to *Dedicated SDNS*. From this point forward, everything seen in the GUI comes from FortiGuard.

FortiManager only works for FortiManager 3000 series and above.

About this document

This document describes how to configure and manage your FortiManager Secure DNS system.

This document assumes you have already connected your FortiManager to the network with the appropriate IP, routing and other information. If not, refer to the FortiManager 5.4.2 Administration Guide.

Licensing

Requirements

In order to use the SDNS configuration on your FortiManager, you will need to request and purchase a license from FortiCare.

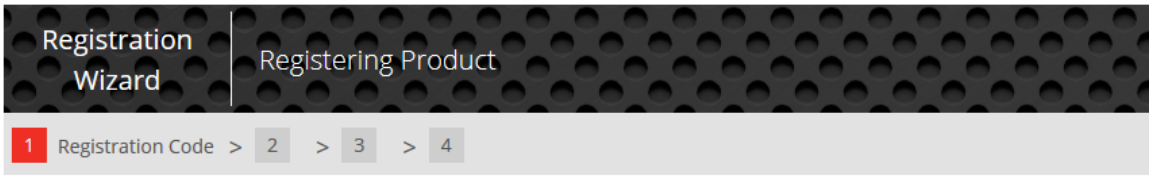
After purchasing a license from FortiCare, you will need to register your product.

Registration

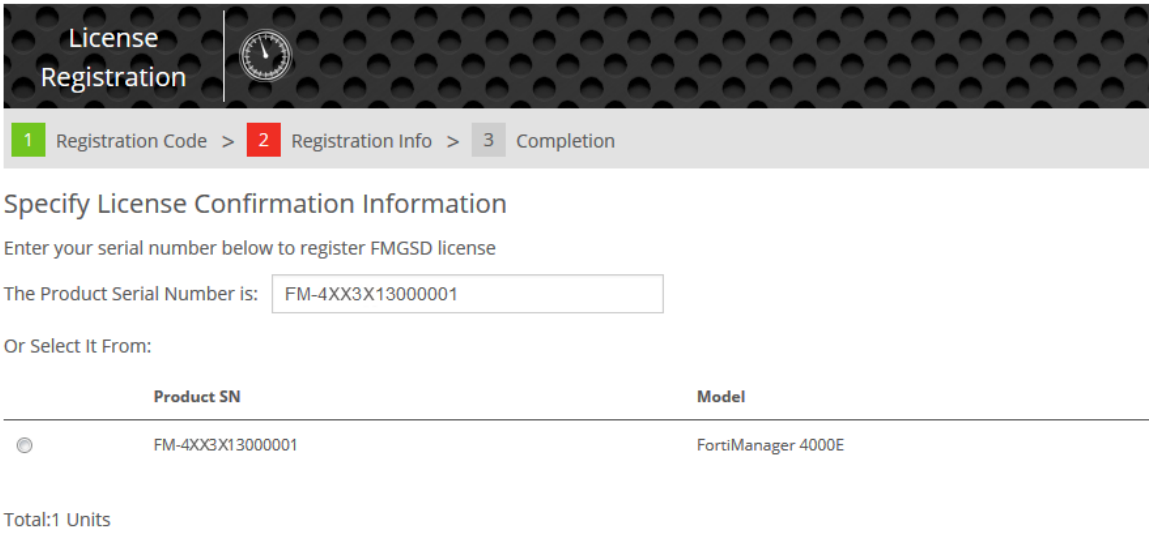
To register your product:

1. Login to *Fortinet Customer Service & Support*.
2. Go to the *Asset tab* > *Product Registration*.
3. Configure the information in the *Registration Wizard*.

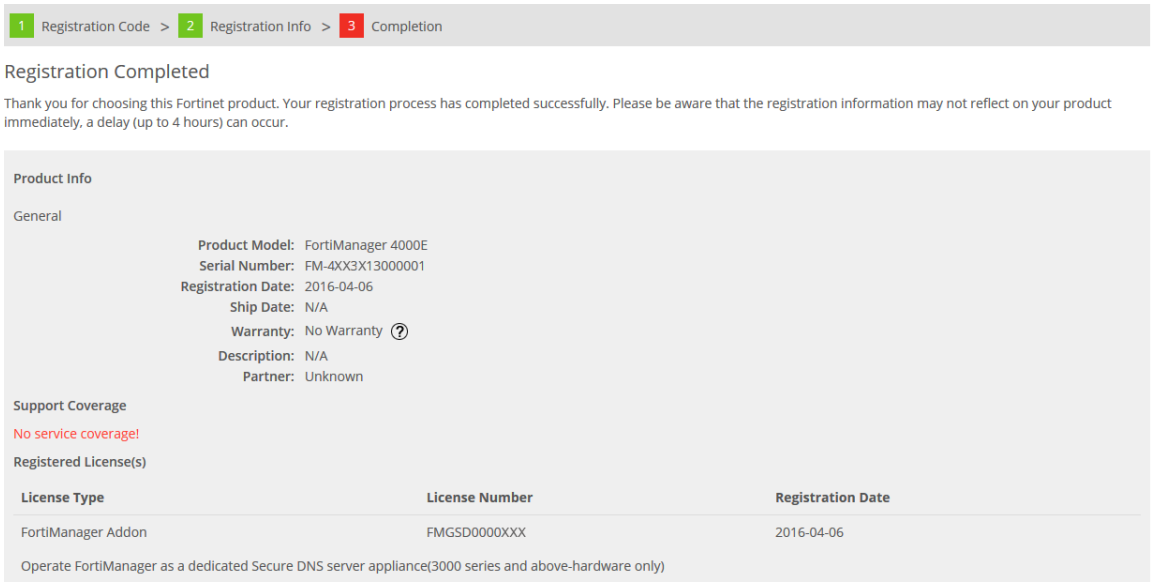
a. Specify the *Registration Code*.



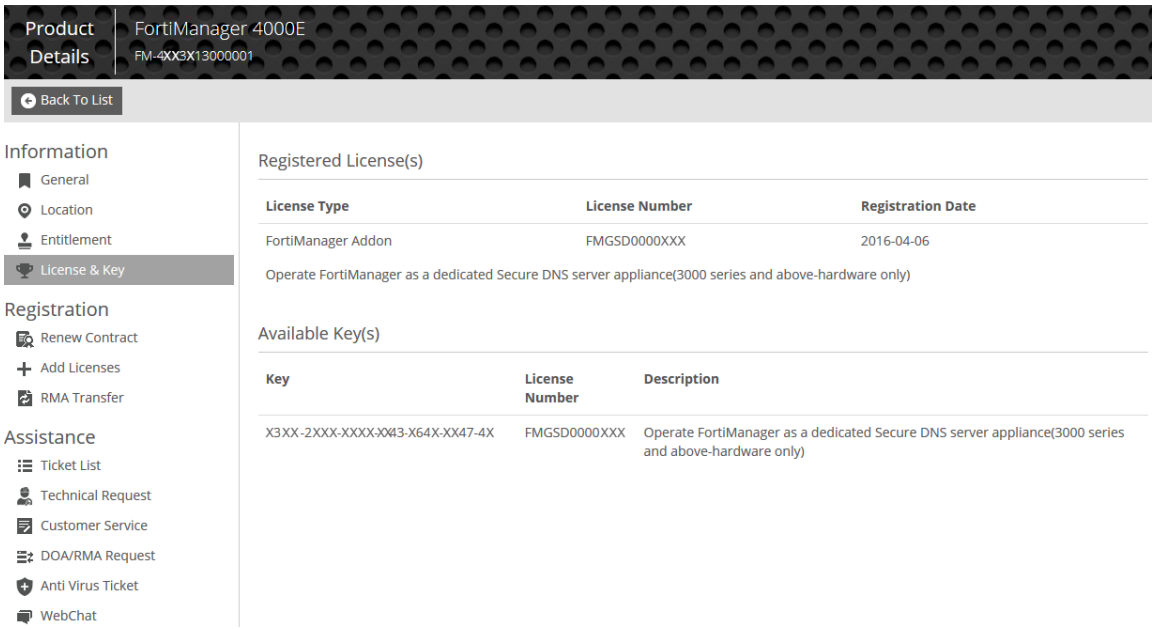
b. Specify the *License Confirmation Information*.



c. Complete registration.



d. View *Product Details and Registered Licenses*.


Product Details
FortiManager 4000E
FM-4XX3X13000001
Back To List
Information
General
Location
Entitlement
License & Key
Registration
Renew Contract
Add Licenses
RMA Transfer
Assistance
Ticket List
Technical Request
Customer Service
DOA/RMA Request
Anti Virus Ticket
WebChat
Registered License(s)
License Type
License Number
Registration Date
FortiManager Addon
FMGSD0000XXX
2016-04-06
Operate FortiManager as a dedicated Secure DNS server appliance(3000 series and above-hardware only)
Available Key(s)
Key
License Number
Description
X3XX-2XXX-XXXX-X43-X64X-XX47-4X
FMGSD0000XXX
Operate FortiManager as a dedicated Secure DNS server appliance(3000 series and above-hardware only)

Installation

Installing the SDNS image in FortiManager

After purchasing the license, you will need to contact Fortinet Customer Service & Support to download the FortiManager Secure DNS image. Then, you can load the FortiManager Secure DNS image to FortiManager from the GUI or CLI.

To enable the SDNS image via GUI:

Steps are needed.

To enable the SDNS image via CLI

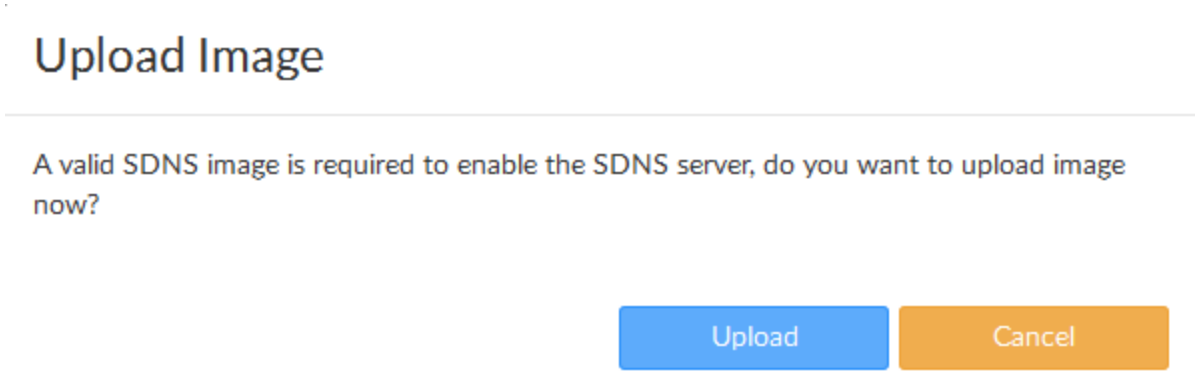
1. Open the CLI console
2. Enter the following command:

```
[FMG Model] # exec sdns
enable Enable and reboot to SDNS system
image Load SDNS image

Example:
FMG4000E Xexec sdns image ftp SDNS-FMG-rls-2.5.0-0005-64bit.out 10.2.78.14 1111 qa1234
Loading image...
Transferred 33.982M of 33.982M in 0:00:03s (10.268M/s)
```

Enabling SDNS in FortiManager

1. Go to *System Settings* > *License Information* widget.
2. Click the *Enable SDNS* button in the Secure DNS Server field.



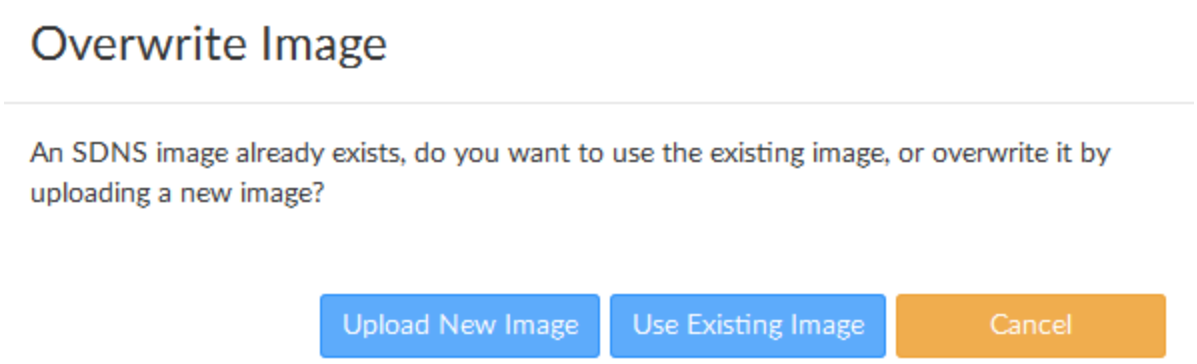
3. Select an SDNS image.
4. Click *Upload*.

FortiManager will reboot. You will need to reconfigure your IP and routing information inside FortiManager. See Configuration for more information.

Already have a SDNS image enabled

If you already have a SDNS image enabled, you have the following options:

Upload a New Image	Upload a new image to overwrite the previously enabled image.
Use Existing Image	Enable the SDNS server and your FortiManager will reboot.
Cancel	Exit the window.



To switch back to FortiManager from SDNS, see "System" on page 14.

Configuration

After applying the license key into FortiManager, your FortiManager will reboot. You will need to reconfigure your settings inside FortiManager Secure DNS. For more details on how to configure your settings, see Settings.

Settings

The following describes the FortiManager Secure DNS settings.

Network

Go to *Settings* > *Network* to configure and manage network interfaces.

To configure network and gateway configurations

You will need to execute the following commands then reboot the SDNS server.

```
/data/etc # ls
```

cat_ big5.txt	cat_ en.txt.4	cat_ fr.txt.7	cat_ jan.txt.4	cat_ kr.txt.7	fdn.conf	network	rclocal_ default
cat_ big5.txt.1	cat_ en.txt.5	cat_ gb.txt	cat_ jan.txt.5	cat_ pg.txt	fdn.conf_ default	network_ default	resolv.conf
cat_ big5.txt.4	cat_ en.txt.6	cat_ gb.txt.1	cat_ jan.txt.6	cat_ pg.txt.7	gateway	nsswitch.conf	resolv.conf_ default
cat_ big5.txt.5	cat_ en.txt.7	cat_ gb.txt.4	cat_ jan.txt.7	cat_ spa.txt	gateway_ default	nsswitch.conf_ default	services
cat_ big5.txt.6	cat_ fr.txt	cat_ gb.txt.5	cat_ kr.txt	cat_ spa.txt.1	hosts	ntp.conf	services_ default
cat_ big5.txt.7	cat_ fr.txt.1	cat_ gb.txt.6	cat_ kr.txt.1	cat_ spa.txt.4	hosts_ default	ntp.conf_ default	syslogd.conf
cat_en.txt	cat_ fr.txt.4	cat_ gb.txt.7	cat_ kr.txt.4	cat_ spa.txt.5	httpd_ user.dat	ntpserver	syslogd.conf_ default
cat_ en.txt.1	cat_ fr.txt.5	cat_ jan.txt	cat_ kr.txt.5	cat_ spa.txt.6	ip_ list.txt	ntpserver_ default	timezone
cat_ en.txt.3	cat_ fr.txt.6	cat_ jan.txt.1	cat_ kr.txt.6	cat_ spa.txt.7	logserver	rc.local	user.dat

```
/data/etc # vi network

ifconfig eth0 192.168.70.2 netmask 255.255.255.0
    ifconfig eth0 up
    ifconfig lo 127.0.0.1

/data/etc # vi gateway
    route add -net default gw 192.168.70.1 eth0
```

You will need to login to the SDNS GUI from `192.168.100.100:2400`. Configure the TCP port to `2400`, and SSH login from TCP `4128`.

The following options are available:

Default Gateway		
	IP Address	Enter the default gateway IP address.
	Interface	Select the interface type. You can choose between *eth0-eth5*.
Public IP		
	IP Address	Enter the public IP address.

The following information is displayed:

Name	The interface type.
IP Address	The IP address.
Subnet Mask	The subnet mask.
Administrative Access	Type of administrative access. Options include: • ssh • https • ping
Service Access	Type of service access. Options include: • dns
Enable	The checkmark indicates that the network interface is enabled.

To Add a Network Interface

1. Go to *Settings* > *Network*.
2. Under *Default Gateway*, enter the *IP address* and *Interface*.
3. Click *Apply* to save the settings.
4. Under *Public IP*, enter the *IP address*.
5. Click *Apply* to save the settings.

FortiGuard Server

Go to *Settings* > *FortiGuard Server* to configure the FortiGuard Server settings.

The following options are available:

Server Name or IP	Enter the server name or IP address. You have the option to select *as overwrite server*.
Network Name resolver	Select either *Local* or *DNS Server*. If you select *DNS Server*, you will need to enter the server address.
Log Level	Select the log level type. The options include: • Emergency • Alert • Critical • Error • Warning • Notice • Inform • Debug The default log level type is *Inform*.

To Add a FortiGuard Server:

1. Go to *Settings* > *FortiGuard Server*.
2. Enter the *Server Name or IP Address*. You have the option to have this server *as the overwrite server*.
3. Select the *Network Name Resolver*.
4. Select the *Log Level type*.
5. Click *Apply* to save the settings.

Date and Time

Go to *Settings* >*Date and Time* to configure the time zone, and date and time settings.

The following options are available:

Time Zone		Select the correct time zone from the drop down.
Date and Time		
	Synchronize date and time over the network	Enable to synchronize the date and time over the entire network.
	NTP Server	Enter the Network Time Protocol (NTP) server to synchronize data and time on your computer with a remote time server every 12 hours.

Manually set the date and time of your system	Manually set the *Month*, *Day*, *Year*, *Hour*, *Minute*, and *Seconds*.

To configure the time zone:

1. Go to *Settings* > *Date and Time*.
2. Under *Time Zone*, select the correct *Time Zone* from the drop down.
3. Click *Apply* to save the settings.

To configure the date and time:

1. Go to *Settings* > *Date and Time*.
2. You can either:
   a. Synchronize the data and time on your computer with a remote server by enabling the *Synchronize date and time over the network* option. You will need to enter the Network Time Protocol (NTP) server address.
   b. Manually set the date and time of your system.
3. Click *Apply* to save the settings.

System

Go to *Settings* > *System* to *Restart*, *Shutdown* or *Switch to FortiManager*.

Admin

The following describes the FortiManager Secure DNS administrative settings.

Password

Go to *Admin* > *Password* to create a new password.

To create a new password:

1. Enter your current password.
2. Enter your new password.
3. Enter your new password again to confirm the change.
4. Click *Apply* to save the settings.

Guest User

Go to *Admin* > *Guest User* to manage and configure new guest users.

The following options are available:

New Guest User	Click to add a new guest user.
Delete	Click to delete a guest user.

To add a New Guest User:

1. Go to *Admin* > *Guest User*.
2. Click *New Guest User*.
3. Enter the *Guest Name* and *Initial Password*.
4. Click *Apply* to save the settings.

To delete a guest user:

1. Go to *Admin* > *Guest User*.
2. Find the guest user you want to delete.
3. Click *Delete*.
4. Click *Ok* in the confirmation dialog box to delete the guest user.

Status

In the *Status* page, you will be able to view the current status of the FortiManager Secure DNS.

The following information is displayed:

Serial Number	The serial number of the device.
Firmware	The firmware version of the device.
Build Date	The date the latest build was installed.
Up Time	The up time of the device.

FortiGuard

Go to *Status* > *FortiGuard* to view the total number of FortiGuards and their respective statuses.

The following information is displayed:

SN	The FortiGuard serial number.
Contract Expiry Date.	The date the FortiGuard contract expires.

Data Packages

Go to *Status* > *Data Packages* to view to current status of all Data Packages.

The following information is displayed:

Description	Type of Data Package.
FortiOS	
Category	Category type.
Group	Group number.
Version	Version number.
Date time	The date and time the data package was created.

Log Viewing

Go to *Status* > *Log Viewing* to view specific logs and historical logs.

To view specific logs:

1. Go to *Status* > *Log Viewing*.
2. In the *Log Type* field, select the type of log from the drop down. The options include:
    a. linkd.log
    b. sdns.log
    c. sec.svr.ntp.log
    d. init.log
    e. update.log
    f. misc.log
    g. https.log
3. Select either:
    a. *Online View* to view the logs online
    b. *Download* to download the log file onto your computer

To view *Historical Logs*, click the Historical Logs button located in the top right corner of the content pane.

Query Statistics

Go to *Status* > *Query Statistics* to configure the query statistics settings.

The following options are available:

Data Condition		
	Time Range	Select the daily time range.
	Granularity	Select the time interval the data will be gathered. Options include every: *1 Minute*, *5 Minutes*, *10 Minutes*, *30 Minutes*, and *1 Hour*.
Display Selection		
	Date Types	Select the data types to be displayed. Options include: *Timeout*, *Not Found*, *Potentially Harmful*, and *Normal*.

Tools

In the *Tools* page you can view System Monitor, Network Monitor and Disk Usage data.

System Monitor

Go to *Tools* > *System Monitor* to view Memory, Swap and CPU usage data.

The following information is displayed:

Memory Usage		
	Total	Total memory usage.
	Used	Current memory usage.
Swap Usage		
	Total	Total swap usage.
	Used	Current swap usage.
CPU Usage		
	Percent	Percent of CPU used.
	Time	Percent of CPU used over time.

Network Monitor

Go to *Tools* > *Network Monitor* to view the receiving and sending data.

The following information is displayed:

KB/s	Amount of data received and sent in KB/s.
Time	The time the data is received and sent.
Interface type	Each interface type is color coded. Each interface indicates the rate the data is received and sent, and the total amount of data has been received and sent.

Disk Usage

Go to *Tools* > *Disk Usage* to view disk usage data.

The following information is displayed:

Device	The name of the device.
Directory	The name of the directory.
Total	The total amount of disk usage.
Used	The total amount of disk usage actually used.
Available	The total amount of disk usage still available.

FORTINET®

High Performance Network Security